24/7 Cyber Incident Response

The Evolving Cyber Threat Landscape

Organisations of all sizes face a wide range of cyber threats, including ransomware, insider threats, and targeted phishing campaigns. Attackers increasingly use artificial intelligence and machine learning to bypass traditional security controls, making threats more complex and more frequent.

24/7 Detection

In this high-risk environment, 24/7 detection and response capabilities are no longer optional, they are essential for organisational resilience.

Book a 30-minute CIR Readiness Call
Request pricing | Start a 30-day PoV

Ekco's **Cyber Incident Response** (CIR) Service provides a certified expert CIRT team on standby around the clock, acting as an extension of your security function during incidents.

Why choose Ekco

- Since 2020, Ekco has helped over 200 organisations recover from critical cyber incidents.
- Played a key role in restoring three major Irish hospitals during the 2021 HSE cyber attack.
- Supported by SANS certified cyber security experts.
- Strategic partnerships with CrowdStrike and Microsoft.
- Rapid response SLAs for fast containment and minimal impact.
- Experience across environments ranging from single devices to over 100,000 endpoints.

Powered by CROWDSTRIKE CREST PEN TEST SOC

How does it work?

Emergency Incident Response

Rapid onboarding with Immediate access to expert Forensic Investigators for rapid triage, containment, and eradication of threats, guiding your organisation through every step of recovery.

Incident Response Retainers

With our Incident Response Retainers, we're already familiar with your environment, enabling faster containment and resolution when incidents occur.

Cyberattack Simulations

Collaborate with expert responders to simulate cyberattacks, test your plans, and boost your team's readiness for real-world incidents.

Reviews & Assessments

Strengthen your organization's cyber resilience with our comprehensive review and assessment services. We help ensure your preparedness for evolving threats by evaluating key components such as Incident Response (IR) Plans, Business Continuity (BCP) Plans, and overall compromise readiness.

Beyond Detection

Our incident response team are equipped with sophisticated technologies and is staffed by highly experienced cybersecurity analysts who possess the knowledge and skills to proactively detect, analyse, and respond to potential threats. We have flexible annual IR Retainer packages covering Essentials, Standard and Premium Service levels that align to SLA's as we understand that a rapid response is critical to containing and limiting the impact of a Cyber Incident.

Complete Recovery

While the immediate containment and eradication of cyber threats are paramount, the journey to full recovery and enhanced resilience often extends far beyond the initial incident response. Many incident response firms conclude their engagement once the direct threat is neutralized, leaving organisations to navigate the complex and critical rebuild phase on their own. Ekco differentiates itself by offering comprehensive advisory services that go beyond incident handling.

Incident Response

Rapid Containment | Forensic Analysis | Eradication

Incident Recovery

Rebuild & Recovery | Remediation & Enhancement

Retainer Levels